Office of the Governor
State Chief Information Officer

SECURITY

Chapter 7 – Controlling E-Commerce Information Security

Scope: These standards apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, “State Information Technology Services.”

Statutory Authority: N.C.G.S. 147-33.110

Section 01 E-Commerce Issues

070101 Structuring E-Commerce Systems including Web Sites

Purpose: To protect the State’s information resources when conducting business or providing services via e-commerce.

STANDARD

Agencies that conduct business via e-commerce shall ensure that information transmitted and/or stored and the supporting information technology applications used are protected by appropriate policies, procedures and security measures. In addition, agencies must comply with relevant portions of the State technical architecture, the requirements of the Office of the State Controller, and applicable legal requirements.

GUIDELINES

Considerations for electronic-commerce security include but are not limited to:

- End-to-end encryption while data are in transit.
- Encryption while data are at rest.
- A consistent approach to securing servers in use. Measures taken would include, but are not limited to:
  - ❑ Removing sample files.
  - ❑ Disabling unnecessary services.
  - ❑ Keeping resources, both application programs and operating systems, up to date with patches.
  - ❑ Enforced paths restricting user access to authorized programs and data.

- ❑ Appropriate agreements with information service providers and value-added network providers.

ISO 17799: 2005 REFERENCES

10.9.1	Electronic commerce
11.4	Network access control
12.1.1	Security requirements analysis and specification

070102 Securing E-Commerce Networks

Purpose: To protect the State’s e-commerce systems by securing the networks that support the operation of those systems.

STANDARD

The State’s e-commerce systems and supporting networks shall be secured to prevent and detect intrusion and misuse. The level of monitoring and logging required for systems and networks shall be determined by a risk assessment. Because e-commerce system risks are increased when system users are connecting to the Internet, it is important to monitor and log these systems.

Both e-commerce Web sites and agency networks need appropriate security controls, including:

- Authentication of users.
- Access control rules and rights for users.
  - ❑ Authority levels and permissions.
  - ❑ Proper authorization of content providers.
- Measures to safeguard the confidentiality, integrity and availability of data, such as encryption in transit and/or in storage and monitoring of user IDs.

ISO 17799: 2005 REFERENCES

10.9.1	Electronic commerce
10.10.2	Monitoring system use
11.1.1	Access control policy
11.4	Network access control

070103 Configuring E-Commerce Web Sites

Purpose: To protect State agency e-commerce sites by minimizing risks.

STANDARD

An agency’s e-commerce Web site(s) must be configured with technical controls that minimize the risk of misuse of the site and its supporting technology. The configuration shall ensure that if any confidential data are captured on the site, it is further secured against unauthorized access and/or disclosure.

The configuration of e-commerce Web sites shall include:

- Removal of all sample files included with the default installation.
- Disabling of unnecessary services and applications.

- Application of current application and operating system patches, within business constraints.
- Establishment of user accounts that are set to the least level of privilege that job duties require.
- Maintenance of operating systems in accordance with approved agency information technology security requirements.
- Restriction of the use of root privilege to only when required to perform duties.
- Establishment of normal change controls and maintenance cycles for resources.
- Logging of systems and/or protecting applications through access control methods.
- Use of secure channels, such as SSH or IPSec, for administrative purposes.
- A secure physical environment for e-commerce servers.

GUIDELINES

When implementing e-commerce applications, agencies should consider using:

- End-to-end encryption while data are in transit, if applicable.
- Encryption while data are at rest.
- Limited trust relationships between systems.

ISO 17799: 2005 REFERENCE

10.9.1	Electronic commerce

070104 Using External Service Providers for E-Commerce

Purpose: To protect the State's interest when using external serve providers for e-commerce solutions.

STANDARD

When agencies contract with external service providers for e-commerce services, the services shall be governed by a formal agreement. In order to support service delivery, the agreements shall contain, or incorporate by reference, all of the relevant security requirements necessary to ensure compliance with the agency's record retention schedules, its security policies, its security standards, and its business continuity requirements.

ISO 17799: 2005 REFERENCES

6.2.1	Identification of risks related to external parties
6.2.3	Addressing security in third party agreements
10.9.1	Electronic commerce
12.5.5	Outsourced software development

HISTORY

Approved by State CIO: March 22, 2006
Original Issue Date: March 22, 2006
Subsequent History:

Standard Number	Version	Date	Change/Description

Old Security Policy/Standard	New Standard Numbers
There are no old security policies or standards that correspond to this chapter.	